CLAIMS

Sub a3

1. A method for authenticating a printed document comprising the following steps:

a) a document producer sends information to be included in a document to an authentication authority;

b) the authentication authority cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer;

c) the document producer prints the document, including both the information and the authentication code; and

d) a document checker cryptographically checks the authentication code against the information in the document.

2. A method according to Claim 1 wherein the document producer includes a bar code in the document, said bar code containing the authentication code, and wherein the document authenticator is provided with means for reading the bar code to obtain the authentication code.

3. A method according to Claim 1 wherein the document includes a pre-printed serial number, which is sent to said authentication authority, and wherein said authentication authority uses said pre-printed serial number in generating said authentication code.

4. A method according to Claim 3 wherein said pre-printed serial number is included in said document as a pre-printed bar code.

5. A method according to Claim 4 wherein the document producer uses a combined printer and bar-code scanner to read said pre-printed bar code and then to print said document.

6. A method according to Claim 1 wherein said document checker performs the following steps:

a) entering said authentication code into a computer;

b) entering information in the document into the computer;

c) causing the computer to cryptographically generate a check code from said information; and

d) causing the computer to compare said check code with said authentication code and to generate a warning indication if said check code does not correspond with said authentication code.

7. A method according to Claim 1 wherein said authentication authority cryptographically generates said authentication code using a cryptographic key associated with said authentication authority.

8. A method according to Claim 7 wherein said cryptographic key is a secret key known to both the authentication authority.

9. A method according to Claim 8 wherein said authentication code is generated by performing a key-dependent one-way hash of said information, using said secret key.

10. A method according to Claim 7 wherein said authentication authority generates said authentication code using the private key of a public/private key pair, and wherein the document checker checks the authentication code using the public key of said public/private key pair.

11. A method according to Claim 1 wherein communication between said document producer and said authentication authority is protected by encryption.

12. A method according to Claim 1 wherein the document producer can specify an option of having the certificate printed by said authentication authority instead of printing the certificate locally.

13. Apparatus for authenticating a printed document, comprising:

a) a plurality of document producer stations;

b) at least one authentication service; and

c) a plurality of document checker stations;

d) wherein each document producer station includes means for inputting information to be included in a document, and means for sending said information to said authentication service;

e) wherein the authentication service includes means for cryptographically generating an authentication code from this information, and means for sending the authentication code back to the document producer staion;

f) wherein each document producer station includes means for printing the document, including both the information and the authentication code;

g) and wherein each document checker station includes means for cryptographically checking the authentication code against the information in the document.

14. Apparatus according to Claim 13 wherein each of said document producer stations includes a combined printer and bar code scanner for reading from said document a pre-printed bar code containing a serial number.

15. Apparatus according to Claim 13 wherein each of said document producer stations includes means for printing bar codes on documents, and wherein each of said document checker stations includes a bar code reader for reading bar codes from documents.